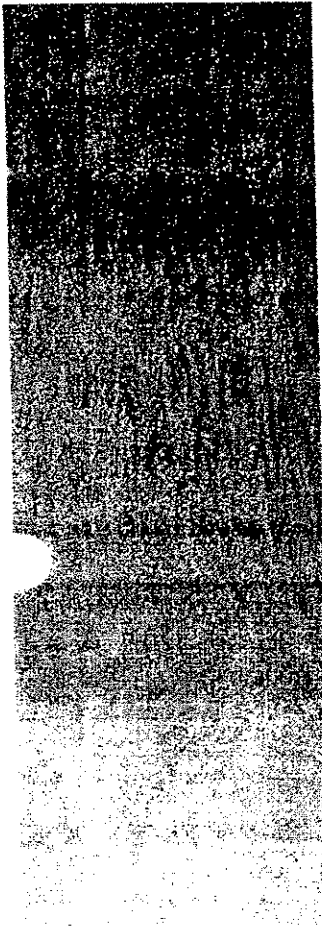


N



INTERNET
SECURITY
SYSTEMS®

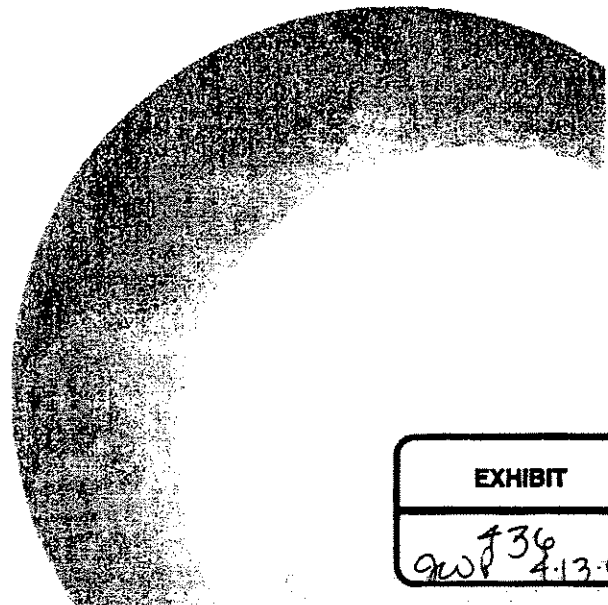


INTERNET|SECURITY|SYSTEMS®

proventia network
Anomaly Detection System

User Guide

Version 3.5



EXHIBIT

436
9w 4.13.06

Internet Security Systems, Inc.
6303 Barfield Road
Atlanta, Georgia 30328-4233
United States
(404) 236-2600
<http://www.iss.net>

© Internet Security Systems, Inc. 2003-2006. All rights reserved worldwide. Customers may make reasonable numbers of copies of this publication for internal use only. This publication may not otherwise be copied or reproduced, in whole or in part, by any other person or entity without the express prior written consent of Internet Security Systems, Inc.

The following applies to portions of this document:

© 1999 - 2006 Arbor Networks, Inc. All rights reserved. Proprietary and Confidential.

Patents pending.

Internet Security Systems and SiteProtector are trademarks and service marks; the Internet Security Systems logo and Proventia are registered trademarks and service marks of Internet Security Systems, Inc. Acrobat and Adobe are registered trademarks of Adobe Systems Incorporated. Check Point, FireWall-1, OPSEC, and VPN-1 are registered trademarks of Check Point Software Technologies Ltd. or its affiliates. Cisco and Cisco IOS are registered trademarks of Cisco Systems, Inc. Microsoft, Windows, Windows NT, and SQL are either registered trademarks or trademarks of Microsoft Corporation. Adaptive Server, SQL, SQL Server, and Sybase are trademarks of Sybase, Inc., its affiliates and licensors. UNIX is a registered trademark in the United States and other countries, licensed exclusively through X/Open Company, Ltd. All other trademarks are the property of their respective owners and are used here in an editorial context without intent of infringement. Specifications are subject to change without notice.

Disclaimer: The information contained in this document may change without notice, and may have been altered or changed if you have received it from a source other than ISS or the X-Force. Use of this information constitutes acceptance for use in an "AS IS" condition, without warranties of any kind, and any use of this information is at the user's own risk. ISS and the X-Force disclaim all warranties, either expressed or implied, including the warranties of merchantability and fitness for a particular purpose. In no event shall ISS or the X-Force be liable for any damages whatsoever, including direct, indirect, incidental, consequential or special damages, arising from the use or dissemination hereof, even if ISS or the X-Force has been advised of the possibility of such damages. Some states do not allow the exclusion or limitation of liability for consequential or incidental damages, so the foregoing limitation may not apply.

Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by Internet Security Systems, Inc. The views and opinions of authors expressed herein do not necessarily state or reflect those of Internet Security Systems, Inc., and shall not be used for advertising or product endorsement purposes.

Links and addresses to Internet resources are inspected thoroughly prior to release, but the ever-changing nature of the Internet prevents Internet Security Systems from guaranteeing the content or existence of the resource. When possible, the reference contains alternate sites or keywords that could be used to acquire the information by other methods. If you find a broken or inappropriate link, please send an email with the topic name, link, and its behavior to support@iss.net.

Document part number: DOC-UG-PROVADS-001-B

March 17, 2006

Contents

Preface	
Overview	vii
How to use Proventia Network ADS Documentation	viii
Conventions Used in this Guide	ix
Getting Technical Support	x
 Part I: Getting Started	
Chapter 1: Introduction to Proventia Network ADS	
Overview	3
Modern Business Problems are Modern Network Problems	4
Proventia Network ADS Architecture	5
Proventia Network ADS Enhances Network Intelligence and Security	7
Chapter 2: Using Proventia ADS Analyzer Web User Interface	
Overview	9
Before You Begin	10
Logging on to the Proventia Network ADS Web User Interface	11
Navigating the Proventia Network ADS Web User Interface	12
Using Navigation Controls	14
Searching in the ADS Web User Interface	17
Chapter 3: Initially Configuring Proventia Network ADS	
Overview	19
How Proventia Network ADS Creates Events	20
Recommended Initial Setup	23
 Part II: Configuring Settings	
Chapter 4: Configuring User Account Settings	
Overview	27
About the User Accounts Page	28
Adding and Editing User Accounts	29
Deleting User Accounts	31
Chapter 5: Configuring SiteProtector Settings	
Overview	33
Configuring SQL Settings	34
Configuring Your ADS Appliance to Communicate with SiteProtector	35
Configuring Passive Host Discovery	36
Chapter 6: Configuring Notification Objects	
Overview	37
About the Notification Objects Configuration Page	38
Notification Types	40
Adding and Editing Notification Objects	41
Deleting Notification Objects	43

Contents

Chapter 7: Configuring Time Objects	
Overview	45
About the Time Objects Page	46
Adding and Editing Time Objects	47
Deleting Time Objects	48
Chapter 8: Configuring Group Objects	
Overview	49
About the Group Objects Configuration Page	50
Adding and Editing Group Objects	51
Importing and Exporting Group Object Files	53
Deleting Group Objects	55
Chapter 9: Configuring Policy Settings	
Overview	57
About the Policy Page	58
How Proventia Network ADS Determines Severity	60
Built-in Behavior Descriptions	62
Built-in Behavior Alerting	64
Configuring Alerting Settings for Built-in Behaviors	65
Configuring Alerting Settings for ATF and User-Defined Rules	67
Configuring Rate Alerting	69
Configuring Active Threat Feed Settings	71
Chapter 10: Configuring Worm Protection Settings	
Overview	73
Configuring Cisco Catalyst 6500 Series Switch Settings	74
Configuring CheckPoint Settings	76
Chapter 11: Configuring Port Objects	
Overview	79
About the Port Objects Configuration Page	80
Adding and Editing Port Objects	81
Importing and Exporting Port Object Files	82
Deleting Port Objects	84
Chapter 12: Configuring General Settings	
Overview	85
Configuring General Settings	86
Exporting and Restoring the System Configuration	87
Chapter 13: Configuring Services	
Overview	89
About the Services Page	90
Configuring Services	91
 Part III: Using ADS	
Chapter 14: Searching Traffic	
Overview	95
About the Explore Page	96
Searching Traffic	98
Searching and Viewing Aggregated Data	102
Viewing Host Relationships	104
Viewing Traffic Flows	106
Creating Group and Port Objects from Traffic	108

Contents

Chapter 15: Managing Policy Rules	
Overview	111
About the Activity Page	112
Viewing Event Details	114
Creating and Editing Rules	117
Enforcing Worm Behaviors	121
Viewing ACLs	122
Chapter 16: Monitoring Network and Appliance Status	
Overview	123
Viewing the Summary Page	124
Viewing Alerts on the Summary Page	125
Viewing a Summary of Network Activity	127
Viewing ADS Status	128
Chapter 17: Viewing Detail Pages	
Overview	131
Viewing Log Details	132
Viewing Details for Hosts and Services	133
Viewing Alert Details	135
Viewing Entity Information	137
Chapter 18: Creating and Viewing Reports	
Overview	139
About the Reports: Create Page	140
Types of Reports	141
Creating Reports	142
Viewing Listed Reports	144
Viewing Reports	146
Managing Scheduled Reports	148
Appendix A: Using PFCAP Expressions	
Overview	151
Searching by Using PFCAP Expressions	152
Example Expressions	155
Glossary	159
Index	163

Contents



Preface

Overview

- | | |
|-----------------------------------|--|
| Introduction | This guide explains how to configure and use the Proventia Network Anomaly Detection System (ADS) appliances and software. |
| Audience | This guide is intended for network security system administrators (or network operators) who are responsible for configuring and managing the Proventia Network ADS on their networks. Administrators should have fundamental knowledge of their network security policies and network configuration. |
| What's new in this release | <p>This release includes support for the Proventia Network Anomaly Detection System appliances. Use the ADS Web user interface to do the following:</p> <ul style="list-style-type: none">• create policy rules• set and enable worm protection settings• configure group, notification, and time objects• import groups from SiteProtector/integrating with SiteProtector• create reports |

Preface

How to use Proventia Network ADS Documentation

Using this guide This guide includes the instructions and information you need to use Proventia Network ADS in the Web user interface. The instructions assume you have completed the installation steps outlined in the Quick Start Guide.

Related publications See the following guides for more information about Proventia Network ADS appliances and this version of the ADS software:

Document	Contents
<i>Proventia Network ADS 3.5 Quick Start Guide</i>	Instructions and requirements for installation and initial configuration of the ADS Analyzer and Collector appliances.
<i>Proventia Network ADS 3.5 Help</i>	Help located in Proventia Manager (or in SiteProtector?)
<i>Proventia Network ADS 3.5 Advanced Configuration Guide</i>	Instructions for optional advanced configuration in the command line interface (CLI).
Readme File	The most current information about product issues and updates, and how to contact Technical Support located at https://www.iss.net/download/ .

Table 1: *Reference Documentation*

Conventions Used in this Guide

Introduction This topic explains the typographic conventions used in this guide to make information in procedures and commands easier to recognize.

In procedures The typographic conventions used in procedures are shown in the following table:

Convention	What It Indicates	Examples
Bold	An element on the graphical user interface.	Type the computer's address in the IP Address box. Select the Print check box. Click OK .
SMALL CAPS	A key on the keyboard.	Press ENTER . Press the PLUS SIGN (+) .
Constant width	A file name, folder name, path name, or other information that you must type exactly as shown.	Save the User.txt file in the Addresses folder. Type IUSR_SMA in the Username box.
<i>Constant width italic</i>	A file name, folder name, path name, or other information that you must supply.	Type <i>Version number</i> in the Identification information box.
→	A sequence of commands from the taskbar or menu bar.	From the taskbar, select Start→Run . On the File menu, select Utilities→Compare Documents .

Table 2: Typographic conventions for procedures

Command conventions

The typographic conventions used for command lines are shown in the following table:

Convention	What It Indicates	Examples
Constant width bold	Information to type in exactly as shown.	md ISS
<i>Italic</i>	Information that varies according to your circumstances.	<i>md your_folder_name</i>
[]	Optional information.	dir [drive:][path] [filename] [/P] [/W] [/D]
 	Two mutually exclusive choices.	verify [ON OFF]
{ }	A set of choices from which you must choose one.	% chmod {u g o a)=[x] [w] [x] file

Table 3: Typographic conventions for commands

Preface

Getting Technical Support

Introduction ISS provides technical support through its Web site and by email or telephone.

The ISS Web site The Internet Security Systems (ISS) Resource Center Web site (<http://www.iss.net/support/>) provides direct access to frequently asked questions (FAQs), white papers, online user documentation, current versions listings, detailed product literature, and the Technical Support Knowledgebase (<http://www.iss.net/support/knowledgebase/>).

Support levels ISS offers three levels of support:

- Standard
- Select
- Premium

Each level provides you with 24-7 telephone and electronic support. Select and Premium services provide more features and benefits than the Standard service. Contact Client Services at clientservices@iss.net if you do not know the level of support your organization has selected.

Hours of support The following table provides hours for Technical Support at the Americas and other locations:

Location	Hours
Americas	24 hours a day
All other locations	Monday through Friday, 9:00 A.M. to 6:00 P.M. during their local time, excluding ISS published holidays Note: If your local support office is located outside the Americas, you may call or send an email to the Americas office for help during off-hours.

Table 4: Hours for technical support

Contact information The following table provides electronic support information and telephone numbers for technical support requests:

Regional Office	Electronic Support	Telephone Number
North America	Connect to the MYISS section of our Web site: www.iss.net	Standard: (1) (888) 447-4861 (toll free) (1) (404) 236-2700 Select and Premium: Refer to your Welcome Kit or call your Primary Designated Contact for this information.
Latin America	support@iss.net	(1) (888) 447-4861 (toll free) (1) (404) 236-2700

Table 5: Contact information for technical support

Getting Technical Support

Regional Office	Electronic Support	Telephone Number
Europe, Middle East, and Africa	support@iss.net	(44) (1753) 845105
Asia-Pacific, Australia, and the Philippines	support@iss.net	(1) (888) 447-4861 (toll free) (1) (404) 236-2700
Japan	support@isskk.co.jp	Domestic: (81) (3) 5740-4065

Table 5: Contact information for technical support (Continued)

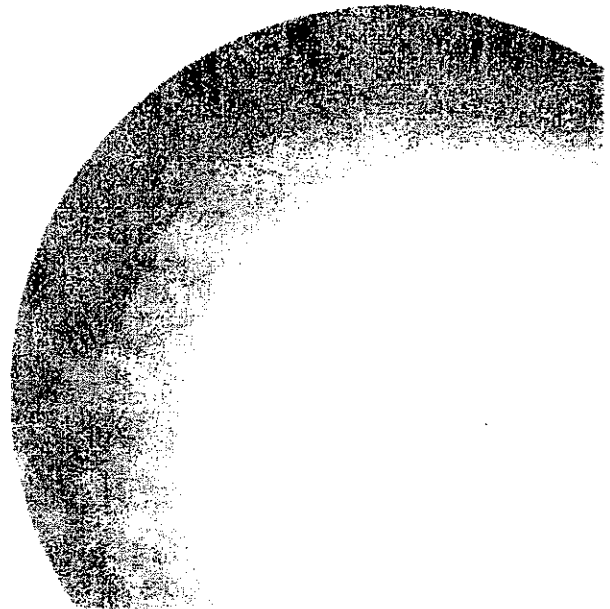
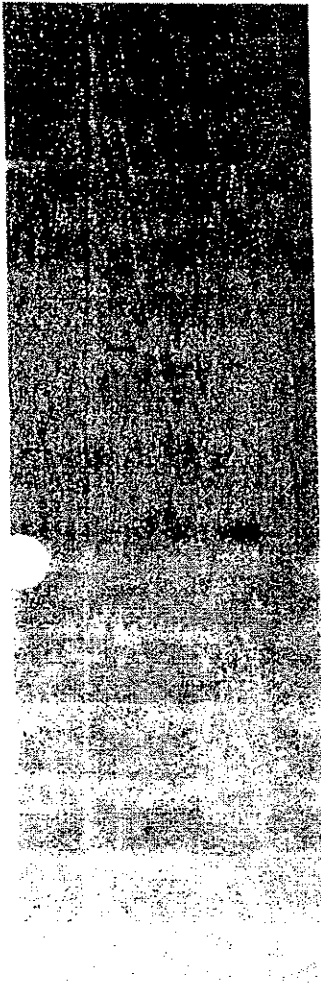
Preface



INTERNET
SECURITY
SYSTEMS®

Part I

Getting Started



Chapter 1

Introduction to Proventia Network ADS

Overview

Introduction This chapter describes the Proventia Network Anomaly Detection System appliances and how they protect your network.

In this chapter This chapter contains the following topics:

Topic	Page
Modern Network Problems	4
The Proventia Network ADS Architecture	5
How Proventia Network ADS Solves Modern Network Problems	7

Modern Business Problems are Modern Network Problems

Introduction

Overall, the networks of large organizations evolve in a chaotic manner due to expansions and reorganizations rather than a carefully executed growth plan. IT organizations often have a well-controlled network backbone, but they cannot maintain complete control of a network organization down to the office switch level without impeding the rapid change necessary in today's competitive environment. Mergers, divestitures, layoffs, and contract employees further complicate tracking and controlling the details of network layout.

Additionally, managing internal networks proves challenging for network administrators dealing with the following:

- insider misuse by disgruntled employees
- zero-day threats
- phishing/pharming
- botnets
- propagating worms
- spyware

At the same time, enterprises must select optimal security solutions that ensure they achieve proper regulatory compliance. Traditional IDS technologies and other perimeter defenses simply cannot address all of these challenges.

Proven Internal Threat Detection and Protection

To meet the demands of today's enterprise IT infrastructures, Proventia Network ADS mitigates threats that target these dangerously unprotected corporate assets and internal resources. When deployed throughout an enterprise network, Proventia Network ADS provides complete visibility and comprehensive protection against the modern network threats that cause the following:

- theft/loss of intellectual property and confidential data
- disruption to business continuity
- brand damage

By discovering and reporting the legitimate relationships between users, machines, and applications, it provides network operators with the situational analysis to know precisely who talks to whom on the network, with what applications, during both on and off hours. Using this information, network operators gain a comprehensive view into traffic shifts, floods, off-hours application usage, and unauthorized network usage and can lock down the network before threats can make an impact.

Proventia Network ADS Architecture

Introduction	<p>Proventia Network ADS provides an overview of network policy and actual operation. The level of detail provided depends on the extent to which you deploy it within your network. Proventia Network ADS Collectors can collect packet capture data, as they are deployed adjacent to important switching stations where they watch the traffic flowing through the switches, either via a shared port on the switch or a network traffic tap. Additionally, they can collect flow data if adjacent routers and switches are configured to export flow data.</p>
Appliance types	<p>There are two types of Proventia Network ADS appliances, you can deploy in one of two modes:</p> <ul style="list-style-type: none">• The Analyzer is a 2U appliance that stores network traffic databases, generates alerts, and provides the primary Web user interface.• The Collectors are 1U appliances that accept and process network traffic data and report summary information to the Proventia Network ADS Analyzer appliance.
Standalone mode	<p>Standalone mode is for smaller deployments in which an Analyzer collects network flow information without using a Collector. In this mode, the Analyzer collects data from up to three flow sources, and accepts raw packet data from network SPAN ports or TAPs.</p>
Two-tier mode	<p>Two-tier mode is for large deployments using both an Analyzer and one or more Collector appliances. In this type of deployment, network flow information and raw packet data from SPAN ports or TAPs is directed to Collector appliances. The Collector appliances then forward consolidated traffic data to an Analyzer appliance.</p> <p>The Collectors can collect information from a variety of flow sources, depending upon the Collector models and the number of Collectors deployed.</p>
Integration with Proventia ESP	<p>Proventia Network ADS provides immediate value to your network as a standalone solution, but also integrates seamlessly with intrusion prevention and vulnerability management systems as a component of the Proventia Enterprise Security Platform (ESP). This integration further helps operators develop and enforce security policies, demonstrate regulatory compliance and harden networks to unauthorized applications and services, while securing mission-critical data and resources.</p>

Chapter 1: Introduction to Proventia Network ADS

Network diagram

The following diagram shows an example of Proventia Network ADS deployed in a network:

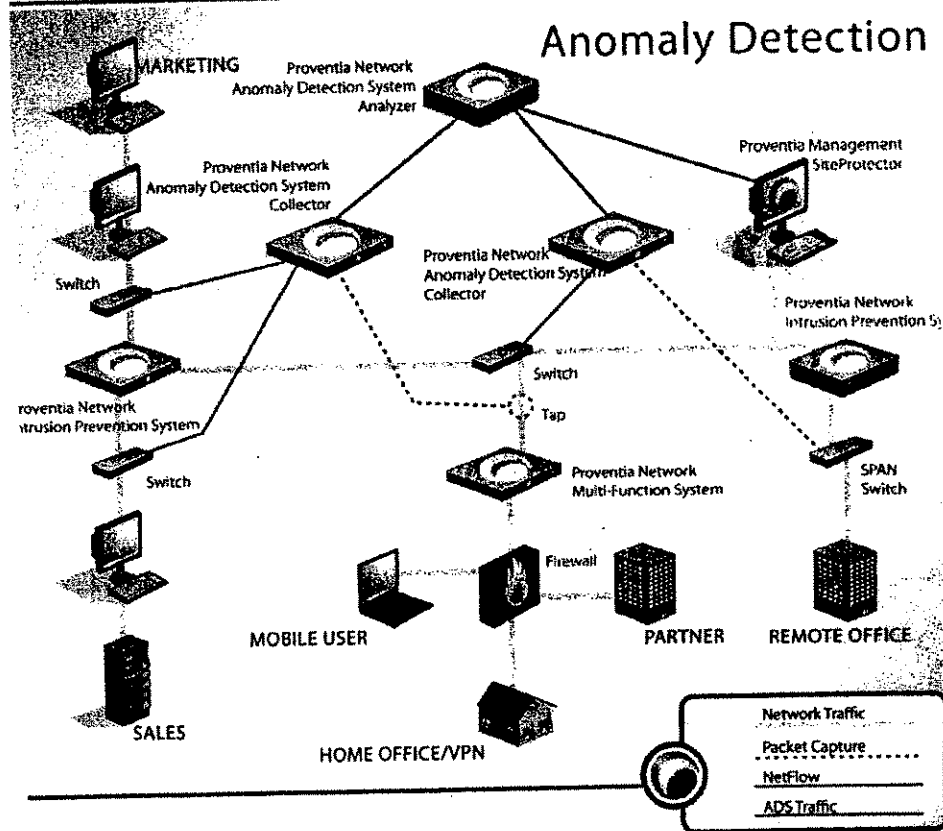


Figure 1: Proventia Network ADS network diagram

Proventia Network ADS Enhances Network Intelligence and Security

Introduction	Proventia Network ADS provides the needed visibility into your network to ensure network integrity and offer the protection of a multi-layered security solution.
Observing traffic and recording flows	Proventia Network ADS operates using a high-level representation of observed traffic. It records individual connections (flows) between clients, servers, and group objects. Proventia Network ADS identifies individual flows using flow rules that capture the significant connection details.
Network policy rules	Policy rules can include client and server IP addresses, client and server ports (for protocols such as UDP or TCP), or ICMP types and codes. These rules describe the network policy—which operations are permitted and which operations are denied within the network.
Segmenting the network through relational modeling	<p>Proventia Network ADS correlates the flow information and identifies which hosts in the network have common behaviors. Behaviors include the use of common flow rules (which correspond to network communication, like fetching Web pages, FTP files, interactive network shell sessions, etc.), status as clients or servers, and traffic patterns.</p> <p>Proventia Network ADS's relational modeling builds a catalog of relationships between every host and service on the network (by inferring them from the network traffic flows) and collects them into aggregates. Any transaction between two network objects indicates a relationship between them. More transactions create stronger relationships. Network operators can view the traffic for these aggregates and divide them further into groups (of clients, servers, or ports) to track traffic or to associate with policy rules.</p>
Observing actual use and alerting for violations	<p>Operators can define the default types of alerts they want the system to create and can start reviewing and updating rules. Additionally, they can create policy from the Search page that shows all traffic for the system, or by searching for specific types of traffic. The system also automatically creates rules for other important events, such as emerging worms, port scans, and host scans.</p> <p>The system then constantly reconciles policy against actual network use. If the traffic violates the policy, Proventia Network ADS generates alerts. As the system detects and reports alerts, network operators can then either decide to act on these detected illegal uses of the network or to adjust the policy, continually refining the use policy.</p> <p>When the system sends alerts, operators can choose to do the following:</p> <ul style="list-style-type: none"> • accept the traffic flow as acceptable use, which creates an accept rule and updates the behavior rule. • forbid the traffic flow, which creates a deny rule and updates the behavior rule. • ignore and delete the alert, which defers changing the policy. <p>Network operators can accept or deny a behavior, either from individual hosts or services, or from a covering aggregate.</p> <p>Example: All members of an engineering group might be clients of the Network File System (NFS) protocol from a group of engineering NFS servers. Rather than having</p>

Chapter 1: Introduction to Proventia Network ADS

individual rules for each pair of clients and servers in the two groups, an operator can accept traffic at the aggregate level by creating a single rule that accepts NFS access from the client group to the server group.

Network operators can also edit policy manually and add rules that correspond to a type of traffic the system has not yet seen, allowing them to actively defend their network before, during, and after worm outbreaks, harden the internal network against future threats, and eliminate insider misuse.

Quarantine against worms

Proventia Network ADS integrates with your existing Cisco Catalyst 6500 Series switches and Check Point firewalls to quarantine worm traffic. Proventia Network ADS's Safe Quarantine solves the worm problem as follows:

- detecting and characterizing worm traffic before it can infect a critical mass of hosts.
- suppressing worm traffic without jeopardizing your critical business processes.
- applying detection and suppression to the internal network as a whole, not just at the perimeter.

Proventia Network ADS examines each network flow and asks its Relational Model if the flow is normal and if the service that is being exploited is normally used. When Proventia Network ADS identifies a worm in the network, it creates a worm policy that allows normal users of the service to communicate, while blocking all of the other traffic on that service. The system then monitors this policy in real-time, and it provides a list of infected hosts that can be used to assist in any clean-up efforts.

Mitigation

Host-to-host wildcard rules are created for each legitimate server on the network. Network operators can preview the ACL rules the system creates. If they have configured enforcement devices, they can also choose to automatically apply the rules on their firewalls and track the quarantined traffic.

Additionally, ADS can create Cisco-style ACLs from the ATF (Active Threat Feed) rules for operators to use, or they can build their own rules to mitigate traffic.

The Proventia Network ADS solution

ISS Proventia Network ADS is the optimal internal solution because it does the following:

- stops known and emerging threats such as zero-day attacks.
- supports proper access for thousands of applications.
- enforces user credentials when accessing resources.
- recognizes appropriate traffic levels when detecting and preventing attacks.
- segments and hardens critical internal network resources from emerging threats.
- scales across the enterprise and leverages existing internal network data sources.
- offers seamless deployment without network redesign or disruption in traffic.
- provides continuous protection through automatic update services (Active Threat Feed).
- generates comprehensive, customized reports for internal and external auditing purposes.

Chapter 2

Using Proventia ADS Analyzer Web User Interface

Overview

Introduction

This chapter describes how to log on and start using the Proventia ADS appliances. The Proventia Network ADS Analyzer provides the Web user interface for all of your ADS appliances. Use the Web user interface to manage your ADS deployment, including creating and managing network security rules and changing administrative settings.

In this chapter

This chapter contains the following topics:

Topic	Page
Before You Begin	10
Logging on to the Proventia Network ADS Web User Interface	11
Navigating the ADS Web User Interface	12
Using Navigation Controls	14
Searching in the ADS Web User Interface	17

Before You Begin

- Introduction** This topic discusses the steps you must perform before you can access the Web user interface for your ADS Analyzer appliance.
- Initial requirements** Make sure you have completed all of the initial configuration steps in the Quick Start Guide for your appliance. Verify that you have done the following:
- connected and configured your Analyzer appliance
 - connected and configured your Collector(s)
 - configured SiteProtector integration
 - successfully connected to the Web user interface
- Logging on as a new user** If you are a new user, make sure your administrator has created an account for you and provided an assigned username and password. You should change this password for security purposes.
- Reference:** See "Choosing a secure and acceptable password" on page 29.

Logging on to the Proventia Network ADS Web User Interface

- Introduction** The Analyzer appliance provides the ADS Web user interface for your Proventia ADS deployment. This topic explains how to log on to the ADS Web user interface.
- Procedure** To log on to the Proventia ADS Web user interface:
1. Open your Web browser.
 2. Type https:// followed by the IP address of your ADS Analyzer appliance.
The Enter Network Password window appears.
Important: You must use a secure connection to access Proventia ADS. Be sure you type https:// in the address bar. If the browser displays an error message about accepting pop-ups, it will not display the page until you accept them.
 3. Right-click, and then select your browser's option for always accepting pop-ups from the Analyzer.
 4. Enter your User Name and Password.
The Proventia Network ADS interface opens, and then the Summary page appears.
- Reference:** See Chapter 16, "Monitoring Network and Appliance Status"
- Troubleshooting** If you are unable to access the Web UI, check to make sure you are logged on to your workstation with a local administrator account, and then try to log on again.

Navigating the Proventia Network ADS Web User Interface

Introduction This topic provides instructions for basic navigation through the Web user interface menus and pages.

About the navigational menu The navigational menu bar on each page displays the current date and time, indicates which menu is active, and allows you to navigate through the Web UI menus and pages.

The Web user interface is divided into the following menu options:

Menu Option	Description
Summary	View a summary of system status.
Explore	Search traffic and create policy rules.
Activity	Manage existing rules, events, and activity.
Reports	Create and view reports of traffic and system data.
Settings	View and change system settings.

Table 6: *Navigational menus*

Navigating between menu options To navigate to a different menu option:

- Click the name of the menu you want to view.
The corresponding page appears.

Navigating to Reports and Settings pages Reports and Settings are menus that contain a list of pages from which you can choose. To navigate to one of these pages:

- Move the mouse over the Reports (or Settings) tab.
- Click the name of the page you want to see from the menu list displayed.

Navigating to the About page The About page displays information about the installed software and hardware, including the version number, build numbers, and the ISS Software License Agreement.

To navigate to the About page:

- Click the copyright link in the lower-right corner of any page in the Web user interface.
- Use the scrollbar to see the ISS Software License Agreement in its entirety.
- Click the copyright notice and 3rd party license link to see the associated licenses.
A window appears that displays all of the copyright notices and licensing restrictions for the software that Proventia Network ADS contains.
- Click the ISS support link to obtain copies of all GPL-based software.
- Close the window to return to the prior page.

Navigating the Proventia Network ADS Web User Interface

Logging off

To log off from the Web user interface:

- Click your browser's Close button from any of the Proventia Network ADS pages.

Using Navigation Controls

Introduction This topic describes the navigation controls that Proventia Network ADS provides to help you access traffic and policy data.

Navigating paged tables The system often displays information in data tables that continue on multiple pages. In these cases, it displays the page number of the page you are viewing in relation to the number of pages that exist (for example, 1/3). It displays the current page number as a text box. You can enter another page number in the text box to navigate directly to that page.

Paging icons The system also displays the following paging icons that allow you to move forward and backward through the pages:

Description	Function
One arrow pointing right (>)	Navigates one page forward.
Two arrows pointing right (>>)	Navigates to the last page.
One arrow pointing left (<)	Navigates one page backward.
Two arrows pointing left (<<)	Navigates to the first page.

Table 7: *Paging icons*

Refreshing pages You can click the refresh icon (⌂) to manually update the page with the most recent event information. On some of the pages, the system displays a check box next to the refresh icon. When you select this check box, the system automatically refreshes the page every two minutes.

Selecting all Many of the tables include check boxes you can use to select specific rows. When the tables include check boxes, the system displays a select all check box in the column header. When you select this check box, the system selects all of the rows in the table on the current page, and acts upon them simultaneously.

Example: To clear all alerts on the Event Detail page, select the select all check box, and then click Clear to delete all of them.

Using the breadcrumb trail Each page in the Web user interface displays a breadcrumb trail at the top, near the page title. The breadcrumb trail shows you where you have navigated by showing the path you have taken. Each page in the trail is a link you can use to quickly navigate back to that page.

Sorting information Some columns allow you to sort the table by those columns. By default, most tables are sorted by severity. The system displays columns that have sorting functionality as links (underlined text). You can recognize the way in which a column is sorted by the up or down arrow that appears next to the column header:

- Columns that contain alphabetical lists are initially sorted in descending alphabetical order, from A-Z. Click an alphabetical column header to re-sort the table by that column in reverse order (Z-A).

Using Navigation Controls

- Columns that contain numerical lists are initially sorted in ascending order. Click a numerical column header to re-sort the table by that specific column in reverse (descending) order.

Using help

When you click the Help button from any of the pages within the Web user interface, a pop-up window appears that contains any relevant information about the page you are viewing. You can move the pop-up window while viewing the page.

Navigation icons

The following table shows the navigation icons and how you use them:











Use this icon...	To do this...
	expand aggregated traffic rows.
	collapse expanded traffic rows.
	toggle timeframe entry format.
	toggle search entry format.
	refresh pages.
	perform an ascending sort: when displayed shows the column in descending order, click to redisplay in ascending order.
	perform a descending sort: when displayed shows the column in ascending order, click to redisplay in descending order.
	navigate to see related traffic flows.
	display a pop-up menu of additional pages you can navigate to, or navigate directly to the entity Info page for that host or service. This is known as the info icon. See the table below for a description of the icon functions.
	expand report data.

Table 8: Navigation icons

Using info icons

The info icon (see table above) displays a menu of choices that correspond to the page you are viewing. The following table shows the menu options for each page on which the icon appears:

Menu Choice	Description	Appears on These Pages
Info	Navigates to the entity Info page.	Alert Detail, Info, Event Detail, Flows, Host Detail, Host Relationships, and Explore.

Table 9: Info icon

Chapter 2: Using Proventis ADS Analyzer Web User Interface

Menu Choice	Description	Appears on These Pages
Limit to	Drills into the selected entity on the current page.	Alert Detail, Flows, Host Relationships, and Explore.
Edit	Navigates to the edit configuration page for the object.	Info, Event Details, Host Details, and Explore.
Explore	Navigates to the Explore page.	Info, Flows, and Host Relationships.
Search	Replaces the current Limit to value with the selected entity.	Flows and Host Relationships.
Connect to	Connects to the selected Web server.	Flows and Host Relationships.

Table 9: Info icon (Continued)

Searching in the ADS Web User Interface

- Introduction** All of the pages that display data tables allow you to search for data within those tables. This topic describes the different ways you can search the database for specific network traffic.
- About search values** Searching allows you to enter values in the Search box that you want the system to match. Search values must correspond to data in the table and can be any of the following:
- case insensitive descriptive text
 - IP addresses
 - CIDR address
- Example:** Search for a specific group object on the Configure Group Object page by entering the group object name and the system displays all matching objects.
- About PFCAP expressions** On the traffic pages within the Web user interface, you can also search using PFCAP expressions. PFCAP expressions allow you to further specify the types of traffic you want the system to match and display.
- Reference:** See Appendix A, "Using PFCAP Expressions" for instructions and information.
- Searching** To search using an expression:
1. Enter the values you want the system to match.
Note: You can enter a name that contains spaces enclose the name in quotes, but you cannot enter names that contain underscores (_).
 2. Click SEARCH.
The system redisplay the page showing all matching values (OR, not AND) with the corresponding page title.
- Selecting the timeframe** The clock icon allows you to change the type of time frame the system uses to match and display traffic. When you click the icon, the system toggles between the time frames. An example of the time frames is shown in Figure 2.

☒ Last: 12 hours ▾

☒ Duration: 12 hours ▾ Starting at: Jun ▾ 27 ▾ 2005 ▾ 07:17 ▾ AM ▾

☒ Between: Jun ▾ 27 ▾ 2005 ▾ 07:17 ▾ AM ▾ and Jun ▾ 27 ▾ 2005 ▾ 07:17 ▾ PM ▾

Figure 2: Timeframes

Chapter 2: Using Proventia ADS Analyzer Web User Interface

About timeframes The following table describes the types of time frames you can select from:

Timeframe	Description
Last	Shows traffic for the last (selected time period).
Duration	Shows traffic for the specified time period, starting from the selected time.
Between	Shows traffic that occurred between a designated range of time.

Table 10: Timeframes

Searching using time frames

To search using a timeframe:

1. Click the clock icon to toggle to the type of time frame you want.
2. To set the **Last** time frame, select the appropriate time period from the list.
The page refreshes and displays traffic for the updated time frame.
3. To set a **Duration**, do the following to set the start time:
 - Select the time period from the list.
 - Select the month in which you want the time period to begin.
 - Type the hour and minutes you want the time to begin in the format HH:MM, and then select AM or PM.
4. To set a range **Between**, do the following to set the start time:
 - Select a month that you want the traffic to begin from the list.
 - Type a number, representing the corresponding day.
 - Select the year from the list.
 - Type the hour you want the range to begin in the format of HH:MM, and then select AM or PM.

Note: You can enter hours as a 24-hour period (for example, 13:00), and the system will ignore the AM/PM box.
5. Repeat Steps 1 through 4 to set the end time.
6. Click **SEARCH**.

Chapter 3

Initially Configuring Proventia Network ADS

Overview

Introduction This chapter briefly describes the steps ISS recommends that you complete in the Web user interface once you have installed Proventia Network ADS.

In this chapter This chapter contains the following topics:

Topic	Page
How Proventia Network ADS Creates Events	20
Recommended Initial Setup	23

How Proventia Network ADS Creates Events

Introduction This topic explains how the Proventia Network ADS determines whether the traffic it detects is an event, and how it generates alerts.

Definition of alerting terms To understand how the system creates events, you should first understand how the following terms are defined within the context of alerting:

Term	Definition
Behavior	Describes a sequence of events that the system is able to match to traffic it detects, equivalent to a signature.
Rule	Consists of a behavior and the response to the behavior.
Alerts (and events)	ADS creates alerts and sends notifications when it observes behaviors on the network that are not allowed. In Site Protector, these alerts show up as "events."
Notification	One of three ways the ADS communicates alert behavior to users: through email, SNMP, and SYSLOG traps. Important: If SiteProtector settings are configured, ADS always automatically notifies SiteProtector when it detects events. If other notification objects are configured, ADS notifies them in addition to SiteProtector.
Policy	A set of rules, the behavior the system is detecting, and the system's response. The ADS uses only one active policy for the network that it monitors.

Table 11: Alerting definitions

Built-in behavior alerting

When you first install Proventia Network ADS, the system monitors your network traffic and gathers traffic data that it uses in building its relational, behavioral models of your network traffic. Based on this data, it generates events for the following built-in behaviors:

- port scans
- host scans
- floods
- worms

You can specify your alerting preferences for these and other types of alerts on the Policy page in the Settings menu. Use the Policy page to define the default alerting settings for both behaviors and system events. Setting alerting defaults before actively using the system makes policy maintenance easier.

Reference: See "Configuring Alerting Settings for Built-in Behaviors" on page 65.

Built-in system alerting

There are two types of alerting profiles that are not associated with rules, but are categorized as system events, Collector Up/Down and Miscellaneous System events. The system uses the Collector Up/Down alert profile to send alerts when the Proventia Network ADS Analyzer stops receiving data from its Collectors and the Miscellaneous System alert profile to send Proventia Network ADS health-related system alerts, such as error conditions and warnings when the software certificate is nearing its expiration date.

How Proventia Network ADS Creates Events

About configuring alerts

You can configure each alert type with its own severity setting, group, time, and notification objects, and add multiple rate alerts for each policy. Add multiple rows of Over, Under, or Profile alerts to associate different alerting thresholds with different time objects. While you may not want to define very specific rates that apply to the built-in alert configuration for all policies, you can do so within a policy itself for any existing policies.

For system-generated behaviors, the system only displays the alerting types that make sense for that type of behavior, but you can add rate alerts for any of the system-generated rules.

How notification and time objects affect rules

Behaviors are affected by two types of configuration objects in Proventia Network ADS, notification objects and time objects. Proventia Network ADS creates an event only if the alert traffic falls within a specified time. These time objects allow you to constrain policy alerting to particular times of the day and week. If the traffic qualifies as an alert, then the system sends alert notifications in the specified formats to the designated recipients.

How group objects affect rules

For many of the behaviors, you can specify which groups you want the system to monitor in conjunction with the alert types you want the system to detect. The system only creates events when the specified group object's members are part of the violating behavior.

Chapter 3: Initially Configuring Proventia Network ADS

Types of alerts

You can define which types of alerts you want the system to detect for each behavior the system is monitoring. The following table describes each alert type and for which behaviors you can enable them.

Alert Type	Description	Alert Categories
Client	Creates an alert when it sees any clients it has not seen before from the selected group involved in traffic.	User-defined, worm, floods, host scans, and port scans
Server	Creates an alert when it detects previously unseen traffic from any servers in the selected group.	User-defined, floods, and port scans
Service	Creates an alert when it sees any new services from any hosts within the selected group involved in traffic.	User-defined, floods, and host scans
Connections	Creates an alert when it sees any out-of-policy connection.	User-defined, floods, and host scans
Host Pair	Creates an alert when it sees traffic between two hosts within the selected group that it hasn't seen before.	User-defined, floods, and port scans
Over Rate	Creates an alert when it sees traffic for this rule that exceeds the configured threshold, over a two-minute interval.	User-defined
Under Rate	Creates an alert when it sees traffic for this rule that drops below the configured threshold, over a two-minute interval.	User-defined
Profile	Creates an alert when it sees traffic for this rule that exceeds the configured threshold, over a two-minute interval.	User-defined

Table 12: Alert types

Note: ATF policies are created as one of the alert categories above, and inherit the settings for the appropriate category.

Alerting icons

The following figure shows how each alert type is represented in the Web user interface on the Policy page:

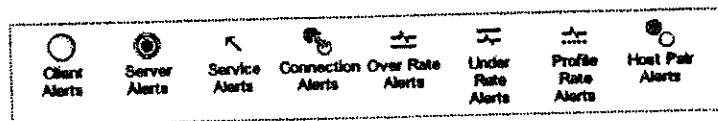


Figure 3: Alerting icons

Recommended Initial Setup

Introduction This topic describes the setup tasks you should complete initially.

Task overview While the system automatically monitors traffic, learns host relationships, and generates certain types of alerts immediately, if you complete these tasks initially, it makes creating and managing policy easier. These steps include:

Task	Where to Find Instructions
Adding notification objects	See "Adding and Editing Notification Objects" on page 41.
Adding time objects	See "Adding and Editing Time Objects" on page 47.
Configuring SiteProtector communication	See "Configuring SQL Settings" on page 34.
Configuring built-in behavior alerting	See "Configuring Alerting Settings for Built-in Behaviors" on page 65.

Table 13: *Initial setup tasks*

How notification and time objects affect policy Behaviors are affected by two types of configuration objects in Proventia Network ADS, notification objects and time objects. Proventia Network ADS creates an event only if the alert traffic falls within a specified time. These time objects allow you to constrain policy alerting to particular times of the day and week. If the traffic qualifies as an alert, then the system sends notifications in the specified formats to the designated recipients.

About notification objects Proventia Network ADS does not come preconfigured with default notification settings, you need to create them on the Notification Object Configuration page in the Settings menu. Once you create a notification specification, the system displays it as a selection choice in default and policy alert configuration.

Proventia Network ADS sends three types of alert notifications: e-mail, syslog, and SNMP traps. You can configure multiple notification objects, which include how you want alerts sent and to whom, on the Notification Configuration page, and then selectively apply them to both user-created and built-in behavior alert configuration.

Initially creating notification objects For each notification object you create, you can include any or all of the three destination types (email, syslog, or SNMP traps). To create a notification object, the system only requires a name, so initially if you know that you will be using the system for remote alerting of some type, but do not have the destination information, you can create an empty object that you can associate with alert configuration now and then further define it when you have the information. You also might want to create different notification groups not only for destination types, but for the destinations themselves. You can configure a notification object for different groups of users, mailing lists, and remote systems and set them up to each receive different types of policy alerts. Proventia Network ADS does not limit the number of notification specifications you can create.

About time objects Time objects are defined as days of the week with an associated time range. Proventia Network ADS comes with one default Time object called All. The All object covers the time period of 24 hours a day, for a full week. Initially, you might want to add other alerting time objects, such as business hours Monday through Friday, for monitoring different network policies. Add these on the Time Objects page in the Settings menu.

Chapter 3: Initially Configuring Proventia Network ADS

Example: Specify business hours as Monday through Friday, from 07:00 to 18:00. You could also describe a weekend, by entering multiple rows, as follows:

- Friday after-hours (18:00 to 00:00)
- Saturday and Sunday (00:00 to 00:00)
- Monday before-hours (00:00 to 07:00)

SiteProtector settings

You can configure your Proventia Network ADS Analyzer to send status and event information to SiteProtector, and query the SiteProtector Database for information.

Reference: See "Configuring SQL Settings" on page 34 for these instructions.

Configuring alerting

Once you have configured notification and time objects, you can define alerting for the built-in behaviors Proventia Network ADS uses to generate alerts.

Reference: See "Configuring Alerting Settings for Built-in Behaviors" on page 65 and "Configuring Alerting Settings for ATF and User-Defined Rules" on page 67.



INTERNET
SECURITY
SYSTEMS®

Part II

Configuring Settings

Chapter 4

Configuring User Account Settings

Overview

Introduction Use the User Accounts page allows you to add, edit, or delete user accounts.

In this chapter This chapter contains the following topics:

Topics	Page
About the User Accounts Page	28
Adding and Editing User Accounts	29
Deleting User Accounts	31

About the User Accounts Page

Introduction The User Accounts page displays all of the configured users in your network. From this page, you can view existing user profiles, see location and login failure information, delete users, and create new accounts.

About user groups User groups allow you to assign one of three different levels of system access to different types of users:

User	Privileges
Administrator	Complete read and write access on all pages.
Analyst	Create and delete policy rules, perform actions that relate to their own user account, and change group and port group objects.
User	Read-only access to most pages, but they can update their own account settings and create and delete their own reports. Cannot do the following: <ul style="list-style-type: none"> • create or delete behaviors or rules • edit rules • edit ATF settings or recreate deleted ATF behaviors

Table 14: User groups

User access on the User Accounts page Analysts and users can update their own account settings, but they cannot view or edit other user account settings. Users with administrative privileges can perform all the actions described in this chapter, except for deleting their own administrator account. An administrator might want to edit a user account to reset a password or to update the user group.

Navigating on the User Accounts page Standard navigation and searching apply on the User Accounts page.
Reference: See "Navigating the Proventia Network ADS Web User Interface" on page 12.

Accounts table The Accounts table shows the following information for each user listed on this page:

Column	Description
User Name	The user name as a link to the Edit Account page.
Real Name	The user's real name.
Group	The user group the user belongs to.
Email Address	The user's email address.
Last Login Location	The IP address for the location the user last used to connect to Proventia Network ADS.
Last Login Time	The time the user last logged onto Proventia Network ADS.
Login Failures	The time the user last tried to log on, but was unsuccessful. This setting is erased when a user successfully logs on to the system.
Delete	Use this check box to delete a user account.

Table 15: User Accounts table

Adding and Editing User Accounts

Introduction	This topic provides the instructions for adding and editing users. Because you add and edit users on the same page, the procedure in this topic applies to both.
User and Analyst Access for Editing Accounts	Non-administrative users can only edit their own user settings on this page. This includes resetting their password or updating their name. Users and analysts are automatically presented with their own user settings when they choose User Accounts from the Settings menu. They do not see the User Accounts table with information about other users.
Choosing a secure and acceptable password	<p>When you add or edit a user account, you should choose a password that contains a sufficient mix of letters and numbers. The password must meet the following criteria:</p> <ul style="list-style-type: none">• Must be at least 7 characters in length.• Must be no more than 35 characters in length.• Cannot be all digits.• Cannot be all lower-case letters.• Cannot include spaces.
Procedure	<p>To configure user settings:</p> <ol style="list-style-type: none">1. Do one of the following:<ul style="list-style-type: none">■ To add a user, move your cursor to the Add a New Account pane.■ To edit a user, click the Username link in the User Accounts table.<p>The system displays the Edit Account pane with the existing user account information.</p>2. Type a unique name in the Username box.<ul style="list-style-type: none">■ The user name must include 1 to 8 characters or numbers or any combination of both.■ Usernames can include hyphens and underscores, but cannot begin with them.■ Usernames cannot include a dot (.) or begin with a number.3. Type the user's first and last name in the Real Name box.4. Select the appropriate user group (Administrator, Analyst, User) from the Group list.5. Type the user's email address as a fully qualified domain name in the Email box.6. Type a password in the New Password box in the Authentication column.<p>Note: As you enter the password, Proventia Network ADS displays the characters on the page as asterisks (*) to hide the password.</p>7. Type the same password again in the Confirm Password box.8. Do one of the following to save the account information:<ul style="list-style-type: none">■ Click ADD to create the account.

Chapter 4: Configuring User Account Settings

- Click **UPDATE** to make changes to an existing account.

The system refreshes the page and displays the new user information in the User Accounts pane.

Important: After you add new users, advise them to change their passwords to maintain security.

Deleting User Accounts

Introduction The Accounts table displays a selection check box in each user row to delete accounts. You cannot delete your own user account.

Procedure To delete a user:

- Select the check box on the user row in the table, and then click **DELETE**.

Chapter 4: Configuring User Account Settings

Chapter 5

Configuring SiteProtector Settings

Overview

Introduction

This chapter contains instructions for configuring your ADS appliance so that it can access data from SiteProtector. These instructions include configuring SiteProtector settings and passive host discovery on your ADS appliance.

In this chapter

This chapter contains the following topics:

Topic	Page
Configuring SQL Settings	34
Configuring Your ADS Analyzer to Communicate with SiteProtector	34
Configuring Passive Host Discovery	36

Configuring SQL Settings

Introduction	This topic contains instructions for configuring Microsoft SQL so that your ADS Analyzer appliance can use it to connect to SiteProtector.
Configuration tasks	To allow the ADS to query SiteProtector for information, you must create a new login for your ADS in Microsoft SQL or Enterprise Manager, and then configure your ADS with that configuration information. You can create new logins using Windows or SQL authentication.
Preferred authentication	For security purposes and easier management, ISS recommends using Windows authentication to connect to SiteProtector. If you use Windows authentication, make sure you set up the same user account permissions that are included in these instructions.
Configuring Microsoft SQL	<p>To configure Microsoft SQL to allow queries from your ADS appliance:</p> <ol style="list-style-type: none"> 1. Start the SQL Server Enterprise Manager. Go to Start → Programs → Microsoft SQL Server → Enterprise Manager. 2. In the navigation pane, click the plus sign (+) to expand the Microsoft SQL Servers node. 3. Click the plus sign (+) to expand the SQL Server Group node. 4. Select (local)(Windows XP or NT). The New Login icon appears as available on the menu bar. 5. Click the New Login icon. The SQL Server Login Properties—New Login window appears. 6. On the General tab, type a name for the Anomaly Detection System to use in the Name box. 7. Select the Windows Authentication or SQL Server Authentication option. <ul style="list-style-type: none"> ■ For Windows authentication, select the appropriate Domain, and then select the Grant access option. ■ For SQL authentication, enter a password in the Password box. 8. Select RealSecureDB from the Database list. 9. Select Default from the Language list. 10. Select the Database Access tab. 11. Select the check box in the Permit column for RealSecureDB. The Database roles for RealSecureDB window appears with public selected. 12. Select the check box for db_datareader. 13. Select the check box for IssApplication. 14. Click OK. Note: For Windows authentication, the username is saved as the domain name followed by the user name. Example: ISS\testuser

Configuring Your ADS Appliance to Communicate with SiteProtector

- Introduction** This topic contains the instructions for configuring the settings on your ADS appliance that allow it to communicate with Site Protector.
- How ADS communicates with SiteProtector** The Analyzer sends status information to the SiteProtector Agent Manager. The Analyzer also sends alert information to the SiteProtector Database and queries the database for information.
- Configuring SiteProtector access on the ADS Analyzer** To configure your ADS to query SiteProtector:
1. Log on to the ADS.
Select Settings→ SiteProtector Settings.
The SiteProtector Settings page appears.
 2. Type the IP address for the agent manager in the SiteProtector Agent Manager box.
 3. Type the IP address for the database in the SiteProtector Database box.
 4. Type the username in the SiteProtector Database Username box.
 5. Type the password in the SiteProtector Password box.
 6. Do one of the following:
 - Click **SAVE** to save the settings.
 - Click **TEST CONNECTION** to test communication between the Analyzer and SiteProtector.
The system displays a message at the top of the page that indicates if the test was successful.
If the test was not successful, edit the settings indicated in the error message, and then test the connection again.
- Important:** ISS strongly recommends that you make changes to the AgentManager settings only from the ADS appliance because of the following:
- If you make changes to the AgentManager settings from the SiteProtector Console, the changes do not appear on the ADS SiteProtector Settings page.
 - The settings made in Proventia Network ADS override any ADS AgentManager settings you have made from the SiteProtector Console.

Configuring Passive Host Discovery

Introduction This topic describes how to configure Proventia Network ADS to automatically discover new hosts from specified groups in ADS and pass them up to SiteProtector. When this happens, they are automatically added to the SiteProtector group you specify.

Before you begin You must configure your ADS Analyzer to communicate with SiteProtector before you can set passive host discovery.

Procedure To configure passive host discovery:

1. Click the group icon, and then select a group from the ADS list.
Proventia monitors this group, and when a newly active host is detected, it adds the host to the group you specify in SiteProtector.
2. Click the group icon, and then select a SiteProtector group from the list.
When your ADS Analyzer detects a new host in the specified group, it will add it to this group in SiteProtector.
3. Click **ADD** to create more rows, and then select the groups you want to watch and add new hosts to.
4. Type the number of days you want the system to wait before considering a client or server to be "new" in the box.
Proventia Network ADS uses this number to determine if the host is newly detected. If it hasn't detected the host in the last number of specified days, it considers it new.
5. Click **SAVE**.

Removing groups from passive host discovery

To remove a set of groups from passive host discovery:

1. Click **REMOVE** on the corresponding row.
2. Click **SAVE**.
ADS stops monitoring that group for new hosts.